United States Patent [19]

Gargiulo et al.

[11] **Patent Number: 4,935,961**

[45] **Date of Patent: Jun. 19, 1990**

[54] **METHOD AND APPARATUS FOR THE GENERATION AND SYNCHRONIZATION OF CRYPTOGRAPHIC KEYS**

[76] Inventors: **Joseph L. Gargiulo**, 5418 Main St., Trumbull, Conn. 06611; **Jose Pastor**, 191 Wilton Rd., Westport, Conn. 06880

[21] Appl. No.: **224,619**

[22] Filed: **Jul. 27, 1988**

[51] **Int. Cl.**[5] **H04L 9/08**

[52] **U.S. Cl.** **380/21**; 380/29; 380/44; 380/45; 380/48; 380/49

[58] **Field of Search** 380/21, 28, 29, 36, 380/43, 44, 45, 48, 49

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,958,081	5/1976	Ehrsam et al.	
3,962,539	6/1976	Ehrsam et al.	
4,004,089	1/1977	Richard et al.	
4,160,120	7/1979	Barnes et al.	
4,172,213	10/1979	Barnes et al.	
4,193,131	3/1980	Lennon et al.	375/2
4,295,039	10/1981	Stuckert	235/380
4,369,332	1/1983	Campbell, Jr.	
4,393,269	7/1983	Konheim et al.	
4,423,287	12/1983	Zeidler	
4,438,824	3/1984	Mueller-Schloer	
4,458,109	7/1984	Mueller-Schloer	
4,531,020	7/1985	Wechselberger et al.	
4,578,530	3/1986	Ziedler	
4,578,531	3/1986	Everhart et al.	
4,588,991	5/1986	Atalla	340/825.31
4,590,470	5/1986	Koenig	340/825.31
4,601,011	7/1986	Grynberg	364/900
4,605,820	7/1986	Campbell, Jr.	
4,607,137	8/1986	Jansen et al.	
4,630,201	12/1986	White	364/408
4,649,233	3/1987	Bass et al.	380/21
4,723,284	2/1988	Munck et al.	380/25
4,731,840	3/1988	Mniszewski et al.	380/21
4,776,011	10/1988	Busby	380/37

OTHER PUBLICATIONS

D. Coppersmith, IBM J. Res. Develop., 2-87, pp. 244-248.

Primary Examiner—Thomas H. Tarcza
Assistant Examiner—Linda J. Wallace
Attorney, Agent, or Firm—Robert H. Whisker; Melvin J. Scolnik; David E. Pitchenik

[57] **ABSTRACT**

A method and apparatus for generating cryptographic keys for a postal manifest and for synchronizing cryptographic keys for transmitting postal data securely on a communication link is presented. The techniques for generating a key and for synchronizing keys use the same apparatus but use slightly different data to create a cryptographic key.

The postal data center maintains a unique set of data for each server station. Using this set of data along with a manifest sequence number (or communication transaction number) and the date, a cryptographic key is created. Each server station stores a fixed master key, KO, a permutation table, Pt, and ID, and GMT date. Using the manifest sequence number (or the communication transaction number) a row of the permutation table is altered and the master key KO is scrambled with the permutation table top get a new key K2. With K2, the date, server ID, and manifest sequence number (our communication transaction number) are encrypted. The result of this encryption yields another key K3. K3 is then used for encrypting the postal manifest or for communicating with a postal data center.

20 Claims, 5 Drawing Sheets

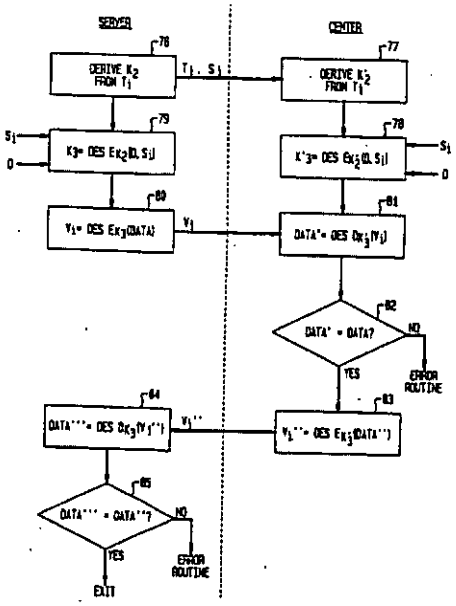


FIG. 1

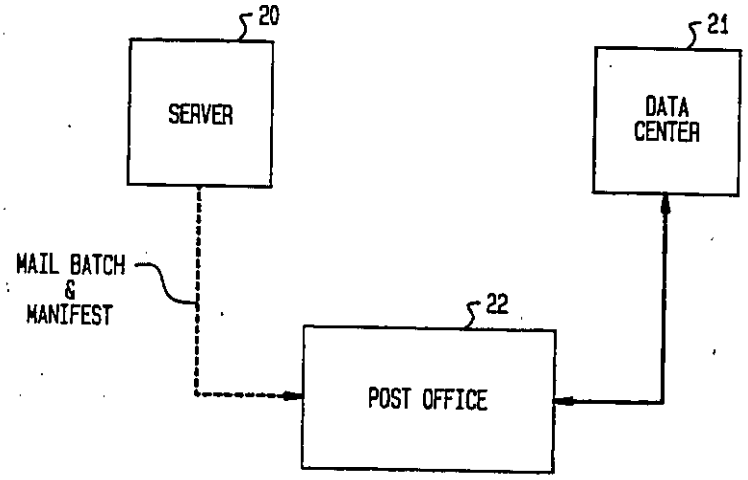


FIG. 2

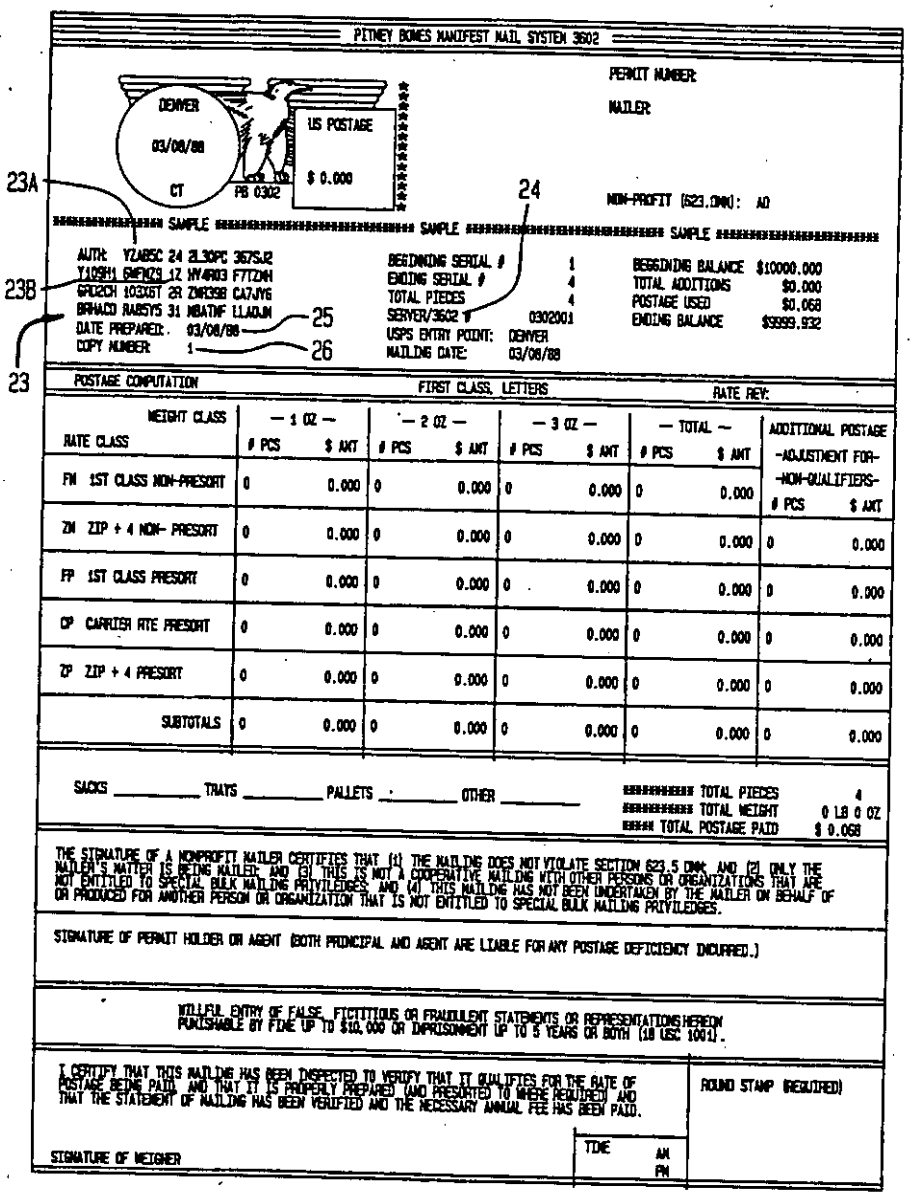
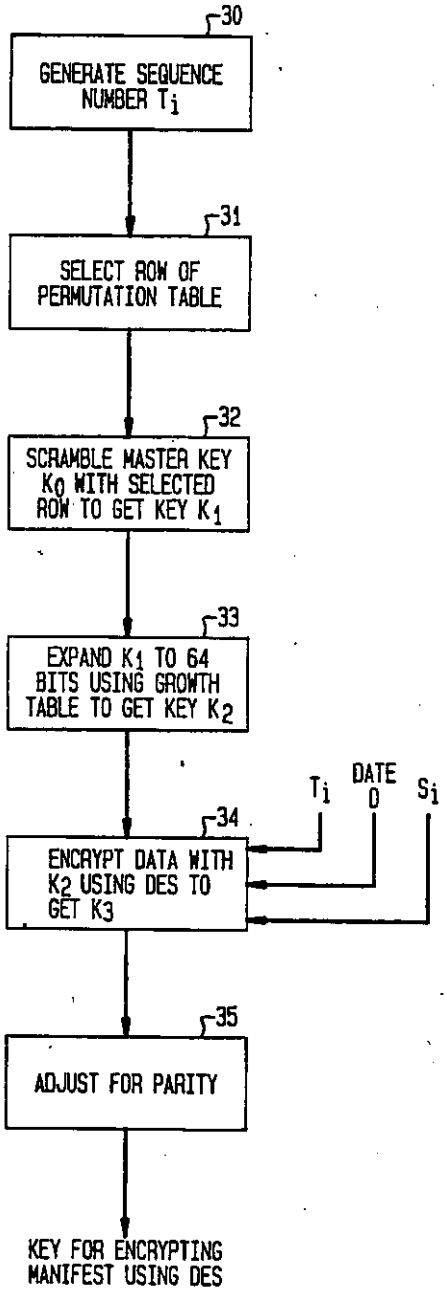

PITNEY BOWES MANIFEST MAIL SYSTEM 3602
PERMIT NUMBER:
MAILER:
DENVER
03/08/88
CT
US POSTAGE
$ 0.000
PB 0302
NON-PROFIT (623.DMM): AD
23A
24
SAMPLE
AUTH: YZABSC 24 2L3OPC 3675J2
Y109H1 6WFNC9 12 HV4R03 F7TZDH
23B
GR02CH 1030ST 2R ZWR39B CA7JY6
BRHACD RA85Y5 31 NBATHF LLADJN
DATE PREPARED: 03/08/88
25
23
COPY NUMBER 1
26
BEGINNING SERIAL # 1
ENDING SERIAL # 4
TOTAL PIECES 4
SERVER/3602 # 0302001
USPS ENTRY POINT: DENVER
MAILING DATE: 03/08/88
BEGGINING BALANCE $10000.000
TOTAL ADDITIONS $0.000
POSTAGE USED $0.068
ENDING BALANCE $9999.932
POSTAGE COMPUTATION
FIRST CLASS LETTERS
RATE REV:
WEIGHT CLASS
RATE CLASS
— 1 OZ —
— 2 OZ —
— 3 OZ —
— TOTAL —
ADDITIONAL POSTAGE
-ADJUSTMENT FOR-
-NON-QUALIFIERS-
PCS
$ AMT
FN 1ST CLASS NON-PRESORT
ZN ZIP + 4 NON- PRESORT
FP 1ST CLASS PRESORT
CP CARRIER RTE PRESORT
ZP ZIP + 4 PRESORT
SUBTOTALS
SACKS _____ TRAYS _____ PALLETS _____ OTHER _____
TOTAL PIECES 4
TOTAL WEIGHT 0 LB 0 OZ
TOTAL POSTAGE PAID $ 0.068
THE SIGNATURE OF A NONPROFIT MAILER CERTIFIES THAT (1) THE MAILING DOES NOT VIOLATE SECTION 623.5 DMM, AND (2) ONLY THE MAILER'S MATTER IS BEING MAILED; AND (3) THIS IS NOT A COOPERATIVE MAILING WITH OTHER PERSONS OR ORGANIZATIONS THAT ARE NOT ENTITLED TO SPECIAL BULK MAILING PRIVILEDGES; AND (4) THIS MAILING HAS NOT BEEN UNDERTAKEN BY THE MAILER ON BEHALF OF OR PRODUCED FOR ANOTHER PERSON OR ORGANIZATION THAT IS NOT ENTITLED TO SPECIAL BULK MAILING PRIVILEDGES.
SIGNATURE OF PERMIT HOLDER OR AGENT (BOTH PRINCIPAL AND AGENT ARE LIABLE FOR ANY POSTAGE DEFICIENCY INCURRED.)
WILLFUL ENTRY OF FALSE, FICTITIOUS OR FRAUDULENT STATEMENTS OR REPRESENTATIONS HEREON PUNISHABLE BY FINE UP TO $10,000 OR IMPRISONMENT UP TO 5 YEARS OR BOTH (18 USC 1001).
I CERTIFY THAT THIS MAILING HAS BEEN INSPECTED TO VERIFY THAT IT QUALIFIES FOR THE RATE OF POSTAGE BEING PAID, AND THAT IT IS PROPERLY PREPARED (AND PRESORTED TO WHERE REQUIRED) AND THAT THE STATEMENT OF MAILING HAS BEEN VERIFIED AND THE NECESSARY ANNUAL FEE HAS BEEN PAID.
ROUND STAMP (REQUIRED)
SIGNATURE OF WEIGHER
TIME
AM
PM

FIG. 3


30
GENERATE SEQUENCE NUMBER T_i
31
SELECT ROW OF PERMUTATION TABLE
32
SCRAMBLE MASTER KEY K_0 WITH SELECTED ROW TO GET KEY K_1
33
EXPAND K_1 TO 64 BITS USING GROWTH TABLE TO GET KEY K_2
T_i
DATE D
S_i
34
ENCRYPT DATA WITH K_2 USING DES TO GET K_3
35
ADJUST FOR PARITY
KEY FOR ENCRYPTING MANIFEST USING DES

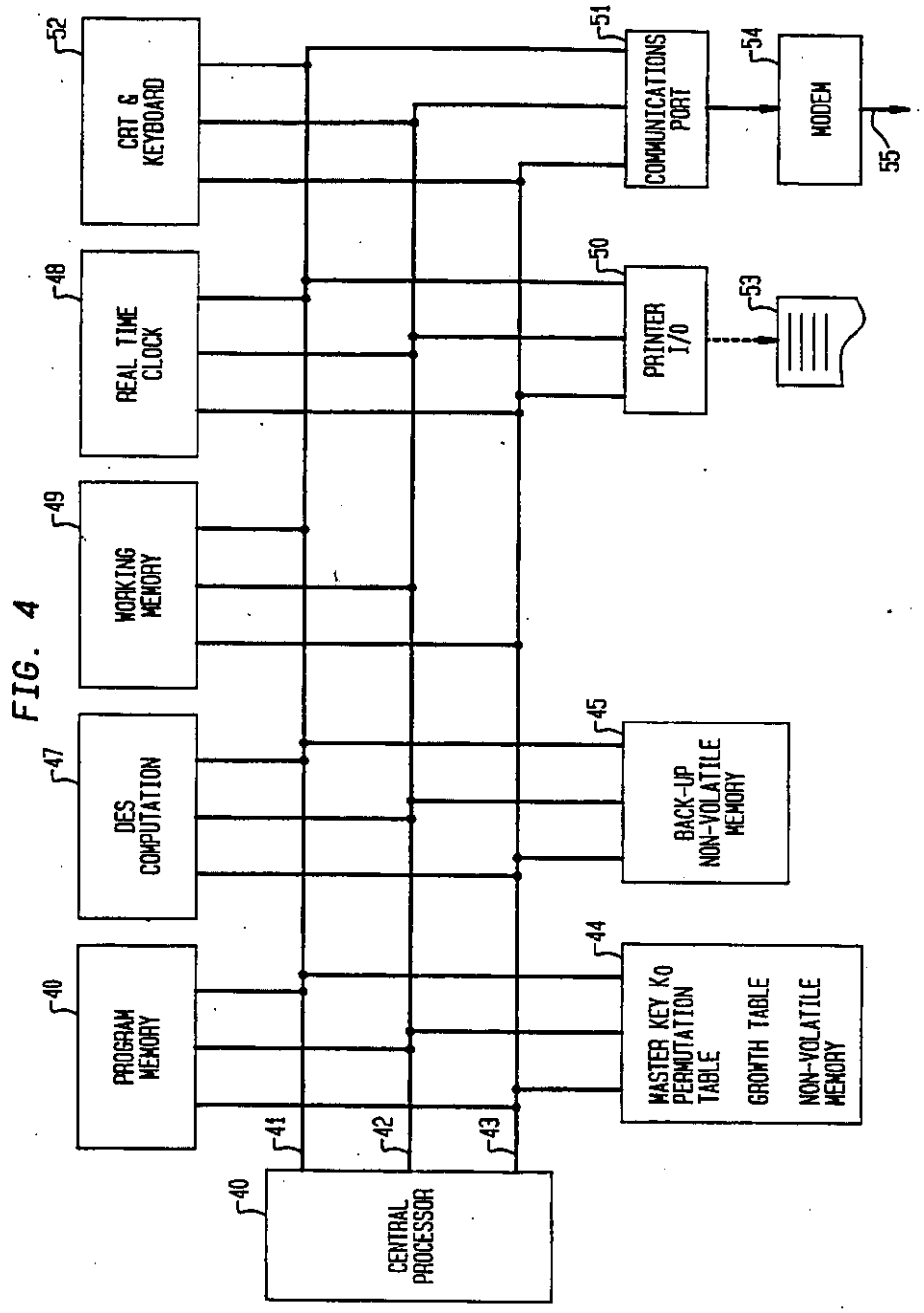
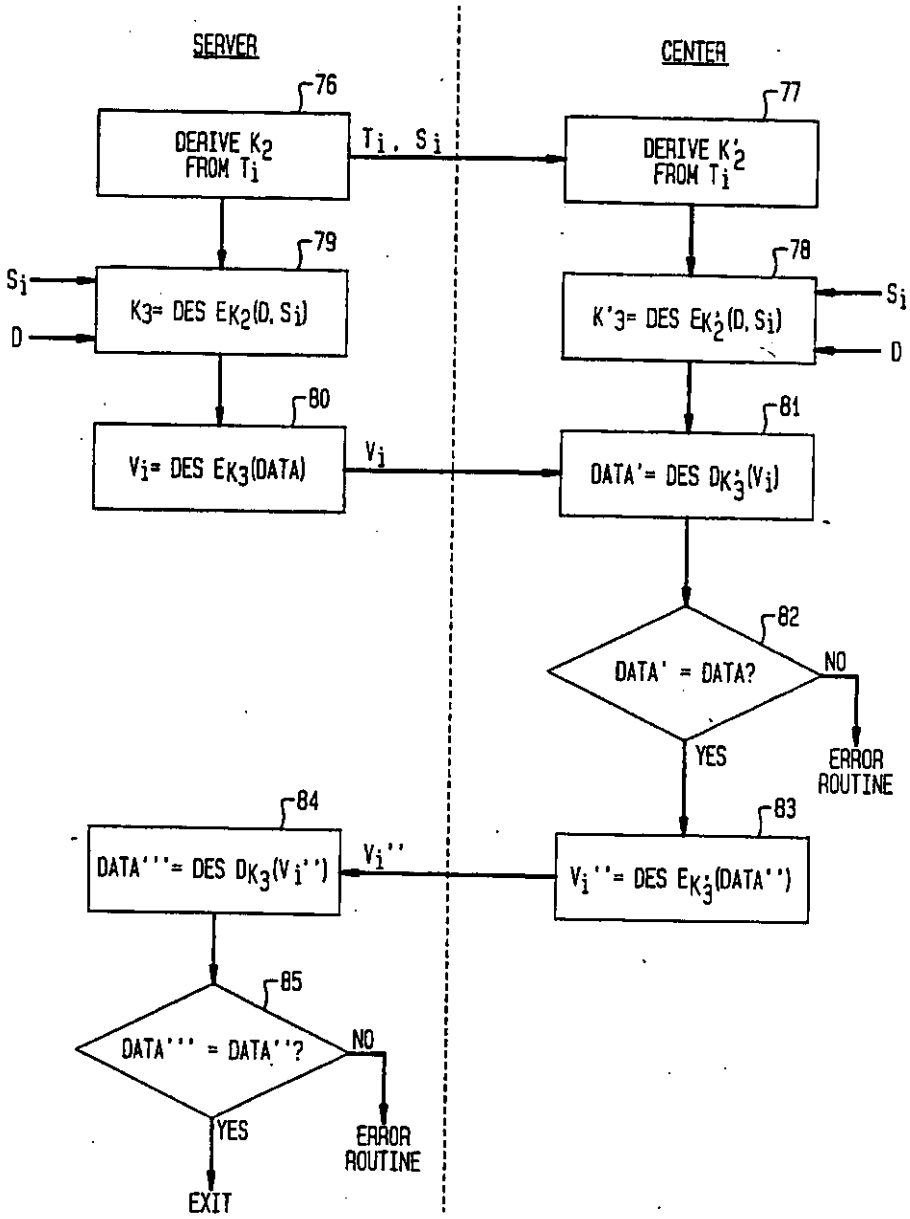

CRT & KEYBOARD
52
REAL TIME CLOCK
48
WORKING MEMORY
49
DES COMPUTATION
47
PROGRAM MEMORY
40
CENTRAL PROCESSOR
40
41
42
43
COMMUNICATIONS PORT
51
MODEM
54
55
PRINTER I/O
50
53
BACK-UP NON-VOLATILE MEMORY
45
MASTER KEY Ko PERMUTATION TABLE
GROWTH TABLE
NON-VOLATILE MEMORY
44

FIG. 4

FIG. 5


SERVER
CENTER
76
DERIVE K_2 FROM T_i
T_i, S_i
77
DERIVE K'_2 FROM T_i
79
S_i
D
$K_3 = DES\ E_{K_2}(D, S_i)$
78
$K'_3 = DES\ E_{K'_2}(D, S_i)$
S_i
D
80
$V_i = DES\ E_{K_3}(DATA)$
V_i
81
$DATA' = DES\ D_{K'_3}(V_i)$
82
DATA' = DATA?
NO
ERROR ROUTINE
YES
84
$DATA''' = DES\ D_{K_3}(V_i'')$
V_i''
83
$V_i'' = DES\ E_{K'_3}(DATA'')$
85
DATA''' = DATA''?
NO
ERROR ROUTINE
YES
EXIT

METHOD AND APPARATUS FOR THE GENERATION AND SYNCHRONIZATION OF CRYPTOGRAPHIC KEYS

This invention relates to the synchronization of cryptographic keys generated at two or more locations without the necessity of passing information between the two locations that could lead to unauthorized determination of the cryptographic keys generated at the locations. While the invention is especially adapted to, and will be specifically disclosed herein, with respect to the provision of a method and apparatus for synchronizing and/or resynchronizing the generation of identical cryptographic keys at the server station and data center of a postal system adapted to monitor the mailing of batch mail, it will be apparent that the invention is not limited to this application.

A server is a mailing machine, for example, for making batch mail, wherein a batch of mail is assembled with a manifest, which serves to identify the contents of the batch to the post office. The manifest has imprinted thereon 20 information such as the quantities of different classes of mail in the batch, etc. In addition, the manifest carries an encrypted verification number to enable the post office to verify the manifest and its accuracy. Each server has an identification number ID (which may be alphanumeric), and the batches assembled by each server are identified by sequential run number T. The ID and run number are printed on the manifest, as well as the date that the manifest was issued.

The system further includes a data center operated, for example, by the Assignee of the present application, that maintains information concerning each server, so that the post office can call the data center to verify each batch that it receives on the basis of information printed on the accompanying manifest.

A problem involved in such a system arises in the difficulty of maintaining cryptographic keys used in the encryption and decryption of the manifest data. While the manifest keys, and the identity of the corresponding servers, may be stored directly at the data center, this technique is cumbersome and requires the storing of an extremely large number of keys at the data center, while still not permitting simple modifications of the keys for increasing the security of the system.

Another problem involved in such a system is securely communicating information between the data center and the server across a data link. To keep this information secure, it is encrypted using the Data Encryption Standard (DES) with a cryptographic key stored by both the data center and server. A further problem arises in initializing the key (for the first time) and secondly, changing the key periodically to increase security. Sending the key across the data link is not acceptable since it could be intercepted and all future transmissions could be decrypted by an information thief.

This second problem is solved by passing a "change key" message across the communication link and employing the technique presented here to create a key on both sides of the link (synchronizing their keys) using Greenwich Mean Time (GMT) date and information contained in the server and data center. Hence, with this technique, the data center and server can synchronize their cryptographic keys without sending critical information across the link.

In accordance with the invention, the data center and server each store an identical 32 bit master key. Remote recharging postage systems conventionally employ a master key of 64 bits, 32 bits of which are fixed and 32 bits of which vary in accordance with certain rules. In order to be compatible with such remote recharging systems, the 32 bit master key of the invention preferably corresponds to the 32 fixed bits of the master key of a remote recharging system. There is no need, however, for the invention to be used in conjunction with such postage recharging systems.

The master key of each server is unique to that server. Since the data center may service a large number of servers, the data center must store the correspondence between the ID of each server and its master key. Thus, upon being informed of an ID, the data center can retrieve the corresponding master keY.

The server and data center each include a real time clock, so that the time of issue of the manifest can be determined. This clock preferably outputs the time as GMT, so that the issue time and date is independent of the location of the server.

The server and the data center each also have stored therein a C column by N row permutation table, wherein C is an integer corresponding to the bit length of the fixed master key and N is an integer of arbitrary length. This permutation table (which may be unique to the server) is used to derive a string K_1 from the master key K_0 of corresponding length. The row of the table that is used for calculation at any time is a function of the transaction number. Each row of the table has a number from 1 to 32 stored at each column, each column corresponding to a bit position of the master key K_0. The string K_1 derived from the permutation table is thus a string of 0's and 1's corresponding to the data at the bit positions of the master key K_0 as identified sequentially by the numbers stored sequentially in the columns of the row of the permutation table corresponding to the current transaction number. The total number of rows N is selected to enable the use of the table for a time commensurate with the expected usage of the table. Preferably the table is not stored as a complete table but in algorithmic form. Thus, preferably data corresponding to one row of the table is stored, along with a secure algorithm for the development of a modified row corresponding to the current transaction number. Storage in this manner provides increased security since the full permutation table is not readily identifiable by examination of the memory. Applicants note that references to selection of a row of the permutation table in accordance with the transaction number and permutation of the master key accordingly are logically equivalent to references to generation of a particular permutation in accordance with an algorithm based on the transaction number and permutation of the master key accordingly, and that such logically equivalent selection is preferred as providing increased security against direct examination of the system memory.

If the master string is shorter than 64 bits, e.g. 32 bits, the server and data center may further include a growth table for expanding the string K_1 to a 64 bit string K_2. This expansion is necessary for compatibility of the key with conventional DES encoding techniques. This table may be a list of 64 numbers, each of the numbers being from 1 to 32 and corresponding sequentially to the bit positions of the 64 bit string K_2. Each bit of the 64 bit string K_2 is a 0 or 1, depending on the data at the bit

position of the 32 bit string K_1 identified by the number in the list.

In accordance with the invention, identical encryption keys can be generated at the server and the data center without the necessity of communication of encryption information between the server and data center, in the following manner.

1. The server determines the row of its permutation table to be used in the calculation, on the basis of the run number. The row to be used may correspond directly to the transaction number.

2. Using the selected row, the server develops a 32 bit string K_1 from the permutation table and the master key K_0, assuming that the master key was a 32 bit key.

3. Using the growth table, the server develops a 64 bit string K_2 from the 32 bit string K_1, and, if necessary, adjusts for parity.

4. The server now encrypts the date from its clock, its ID number, and the run number, with the 64 bit string K_2, to produce a 64 bit encryption key K_3. The encryption may employ the data encryption standard DES.

5. The encryption key K_3 may be adjusted for parity. Those skilled in the art will recognize that the DES standard DES encryption algorithm treats one bit in every byte of the received key as a parity bit and makes actual use of only 56 bits of the key for encryption. Accordingly by "adjusted for parity herein" is meant setting the eighth bit in every byte of the key in accordance with a preselected odd or even parity.

6. The data center receives the ID number and the run number, which are printed in plain text on the manifest, selects the appropriate master key K_0 and permutation table for the identified server, and duplicates steps two through five.

In order that the invention may be more clearly understood, it will now be disclosed in greater detail with reference to the accompanying drawings, wherein:

FIG. 1 is a simplified block diagram of a system for monitoring the mailing of batch mail;

FIG. 2 is an example of manifest that may accompany a batch of mail;

FIG. 3 is a flow diagram illustrating the generation of a cryptographic key in accordance with the invention;

FIG. 4 is a block diagram of a system that may be employed at the server and/or the data center of a postal system for the generation of a cryptographic key, in accordance with the invention;

FIG. 5 is a flow diagram illustrating a method for checking the accuracy of the generation of identical cryptographic keys at two stations.

Referring now to the drawings, and in particular to FIG. 1, therein is illustrated a postal system including a server 20, a data center 21 and a post office 22. The server 20 is provided with facilities for batch mailing, wherein a batch of mail to be mailed is forwarded to the post office 22, along with a manifest providing detail of the contents of the batch, e.g. the totals of different types of mail and different classes of mail, and postage required for the mailing of the batch. In order to verify the manifest, the manifest has imprinted thereon an encrypted number which, when decoded, should verify the various data imprinted on the manifest. A typical manifest for this purpose is illustrated in FIG. 2, wherein a block 23 of characters represents an encryption of various data on the manifest. The manifest further includes an identification number 24 of the server, the data of issue 25 of the manifest, and the run number 26, i.e. the sequential number of the current batch in a series of batch mailings by the server.

Upon receipt of the batch and corresponding manifest, the post office, in normal procedure, communicates with the data center 21, which may be a commercial organization such as the assignee of the present application, and advises the data center of the identity of the server that issued the manifest and the manifest run number as well as a portion 23a of the block 23 of the encrypted numbers. The data center incorporates encryption/decryption programs and data, the same as employed by the server, and upon receipt from the post office of the identification of the server and the run number can regenerate further information appearing on the manifest, or upon receipt of such further information, can regenerate the encrypted numbers. If necessary, upon receipt of the entire block of encrypted numbers, the data center can regenerate for the post office all of the data on the manifest that has been encrypted, for verification purposes.

Further data on the manifest is of a conventional nature, and need not be discussed herein. With respect to the data center, it is of course apparent that it is necessary for the data center to maintain a record of the various keys, tables, etc. employed by each of the servers associated therewith, so that upon receipt of the identification of a server and the transaction number, the pertinent material for encryption and decryption is available for use.

FIG. 3 illustrates a flow diagram showing the generation of a key in accordance with the invention for use in an encryption or decryption process. In accordance with the invention, at block 30, a sequence number T_i is generated in order to determine the row number of the permutation table that is to be employed in a given encryption or decryption. When the number T_i is determined at the server, this step may constitute the stepping of a counter to access the next available row of the permutation table stored therein. When the number T_i is to be employed at the data center, it may be transmitted thereto from the post office upon inspection of a manifest. This communication may be oral, as desired.

After determination of the sequence number, the row of the permutation table corresponding thereto is selected, at block 31. The master key K_0 is then scrambled in accordance with the selected row of the table, to get the key K_1, as indicated at block 32. If it is necessary to expand the key K_1 to render it adaptable for use with an encryption standard such as DES, the key K_1 is expanded by the use of a growth table, at block 33, to produce the key K_2. In order that the final key K_3 be continually varied, one or more data inputs such as the sequence number T_i and/or the date D, and/or the identification number S_i of the server, are encrypted by the K_2, employing DES. This result K_2 is then adjusted for parity at block 35 to produce the key K_3 for encrypting the required data on the manifest, employing for example the DES.

A suitable system for generating a key, in accordance with the invention, is illustrated in FIG. 4. While this system is especially adapted for use in a server, it will be apparent that conceptually the blocks thereof are also adaptable for application to the data center. The system incorporates a central processor 40 of conventional construction, for example, a microcomputer having address, data and control buses 41, 42 and 43 respectivelY. A nonvolatile memory 44 stores the master key K_0, a permutation table P_C, and a growth table G_T.

Preferably the table P_C may be stored in the form of an initial row and a simple, secure algorithm, based on the transaction number, to generate further rows of the table so that the memory **44** need not store the full permutation table. The particular algorithm selected to generate the successive rows of the permutation table is not critical to the subject invention, so long as it is kept secure. For example, it may consist of no more than the successive interchange of pairs of elements in successively generated rows, the pairs being selected in accordance with the transaction number. This technique minimizes the memory space required for the permutation table. In addition, a further memory **45** may be provided as a back-up for the memory **44**.

The memory **46** stores the program for generation of the key, in accordance with the invention, and the subsystem **47** may comprise a chip for effecting DES encryption and decryption. For example, an Advanced Micro Device chip AMD Z8068, or a Motorola chip MC 6859 may be provided for this purpose. DES decryption is discussed for example, in FIPS .

The system of FIG. **4** further includes a real time clock **48** providing an output of the date based upon GMT time. In addition, the central processor is connected to a working memory **49**, a printer I/O **50**, communication port **51**, and a CRT and keyboard **53** to enable manual input and output to the micro-computer, as well as display of the operation of the system. The printer I/0 **50** is coupled to a printer **53** for printing the manifest, and the communications port **51** may be connected to a modem **54**, to enable communication between the server and other device, such as the data center via a communication link **55**.

On occasion, it may be necessary to verify that identical codes are being generated by the server and the data center. A program for effecting such verification is illustrated in FIG. **5**, wherein steps may be effected externally of the server and data center, and do not directly form a part of the present invention. As illustrated, based on a selected transaction number T_i at **76** the server generates a key K_2 in the manner described above, and based upon the same transaction number, at **77** the data center generates a key K'_2 in the same manner. (As used herein "transaction numbers" identify particular communications between a server and the data center. It will be recognized that transaction numbers are used equivalently to "run numbers" to generate keys.) At **79** and **78** respectively the keys K_2 and K'_2 are employed to encrypt the date D and server number S_i employing DES to generate keys K_3 and K'_3. A message V_i is generated by encrypting predetermined DATA at **80** with key K_3. V_i is transmitted to the center and decrypted using key K'_3 at **81**. A communication link, as shown in FIG. **5**, may be employed for transmitting the transaction number T_i server ID, S_i and encrypted data V_i from the server to the data center. The decryption of message V_i, DATA', is then compared at block **82** with the predetermined DATA, which is also stored in the center. If a comparison does not exist, an error has occurred and a request may be made to recheck the calculations. If a comparison is made, then predetermined DATA" (which may be equal to DATA) is encrypted with the use of the key K'_3 at block **83** to generate encrypted message V_i" and passed via a communication link for decryption in a DES decryption step at the server at **84** employing the key K_3. The result is compared with the DATA' stored at the server at block **85**. If a comparison exists, then complete synchronization exists between the server and the data center.

In accordance with the subject invention, a server and data center are provided, which each include:

1. An identical master key K_0 stored in memory. As above discussed, this may be a 32 bit key for convenience in postal systems, or it may have any other number of bits. This key is a secure number, i.e. its identity must be maintained in the equipment or by authorized personnel in complete secrecy.

2. An identical permutation table. The permutation table, an example of which is illustrated in Table 1, has as many columns C as there are bits in the master string to be encoded, e.g. 32 in the present example. The table has an arbitrary number N of rows, the number N preferably being sufficiently large that a separate row can be provided for each transaction that can be expected in a predetermined period of usage of the device. Each row of the table contains numbers (e.g. from 1 to 32), randomly distributed from 1 through C. These numbers correspond to the bit positions of the master string to be encoded. As the term "permutation" is used herein, it is not necessary for each of the numbers from 1 to 32 to be preset in each row, and duplication of numbers is hence permissible.

When a row of the permutation table has been selected, a C bit (e.g. 32 bit) result is generated as a new string in which each bit position of the new string corresponds to the contents of the bit position of the master string addressed at the corresponding column of the permutation table.

Thus referring to the permutation table of Table 1, assuming that the row 2 has been selected, the first bit of the new 32 bit string will be the same as the bit at the third bit position of the master key, the second bit of the new 32 bit string will be the same as the bit at the 27th bit position of the master key, the bit at the third bit position of the new string will be the same as the bit at the 13th bit position of the master string, etc.

TABLE 1

	COLUMN											
	1	2	3	4	5	6	7	8	9	10	...	32
1	3	27	13	15	18	7	4	2	1	30	...	5
2	2	27	13	18	15	7	4	2	1	30	...	5
3	3	27	13	18	15	4	7	2	1	30	...	5
4												
5												
.												
.												
N												

While the permutation table may be stored in the systems in the form of a table, the invention also contemplates algorithmic storage of less information than the complete table, along with suitable algorithms for deriving the required data of any row. Thus, the first row may be stored in memory, along with an algorithm for modification of the first row in accordance with the identity of the transaction number, to derive the data of the row corresponding to the transaction number.

The particular choice of algorithm for modification of the first row is not critical and its selection is not a limitation of the subject invention. For example, as is shown in FIG. **1**, selected pairs of cells may be interchanged cyclically in accordance with Ti.

3. If necessary in the system, a growth table for expanding or diminishing the number of bits of the key,

from K_1 to K_2. When a master key of 32 bits is employed, for example, and it is necessary to expand the key to 64 bits for use in DES encryption, a table such as shown in Table 2 herein may be employed.

TABLE 2

Bit Position	Bit Position Of K_1 From Which Data For K_2 Is Derived
1	31
2	5
3	1
4	12
5	25
.	.
.	.
.	.
64	5

When a growth table as shown in Table 2 is employed, it is evident that the first bit position of K_2 will have the same data as that at the 31st bit position of K_1, the second bit position of K_2 will have the same data as that at the fifth bit position of K_1, the third bit position of K_2 will have the same data as that at the first bit position of K_1, etc.

While the invention has been disclosed and described with reference to a minimum number of embodiments, it will be apparent that variations and modifications may be made therein, and it is therefore intended in the following claims to cover each such variation and modification as falls within the true spirit and scope of the invention.

What is claimed is:

1. A method for generating encryption keys for a sequence of messages comprising the steps of:
   (a) determining a sequence of N different encryption keys;
   (b) associating a value of a sequence variable T_i, with each of said messages; and
   (c) selecting one of said N encryption keys as a function of said variable T_i for each of said messages and encrypting at least a portion of each of said messages in accordance with an encryption key derived in a predetermined manner from the corresponding one of said selected keys; and wherein
   (d) said step of selecting one of said encryption keys produces results identical to the steps of:
      (d1) storing a fixed master key K_o having C elements;
      (d2) storing a permutation table, said table having C columns and N rows, the columns of said table sequentially corresponding to the element positions of key K_0, the elements of said table consisting of numbers from 1 to C; and
      (d3) selecting a row N_i of said table in accordance with said variable T_i; and
      (d4) scrambling key K_o to derive an encryption key K_1, having C elements, by, for all of said elements of K_1, setting the jth element of K_1 equal to the yth element of K_0, where y is the number at column j, row N_i of said permutation table, where j is an integral variable ranging from 1 to C.

2. The method of claim 1 further comprising expanding K_1 in a predetermined manner to derive an expanded encryption key K_2.

3. The method of claim 2 further comprising adjacent K_2 for parity.

4. The method of claim 2 further comprising modifying K_2 to form an encryption key K_3, said step of modifying comprising encryption variable data with K_2 to generate K_3.

5. The method of claim 4 wherein said step of encrypting variable data comprises encrypting a sequence dependent variable.

6. The method of claim 2 further comprising modifying K_2 to form an encryption key K_3, said step of modifying comprising encrypting variable data with K_2 to generate K_3.

7. The method of claim 6 wherein said step of encrypting variable data comprises encrypting a sequence dependent variable.

8. The method of claim 1 further comprising storing said permutation table in algorithmic form.

9. A method for synchronizing the generation of an encryption key K_3 at first and second stations comprising the steps of:
   (a) providing identical sequences of N different encryption keys at said first and second stations;
   (b) selecting a value for a variable T_i;
   (c) selecting one of said N encryption keys in accordance with said selected value and a predetermined function of said variable T_i at each of said first and second stations to obtain encryption keys K_1 and K'_1 respectively;
   (d) encrypting a block of data D at said first station using an encryption key derived in a predetermined manner from said key K_1 to generate a message V_1;
   (e) providing the plain text of said block D at said second station;
   (f) transmitting said message V_i from said first station to said second station;
   (g) decrypting said message V_i using a key derived from said key K'_1 in said predetermined manner to provide a block of data D; and,
   (h) comparing said data D and data D' to verify synchronization at said second station.

10. A method as described in claim 9 comprising the further steps of:
   (i) encrypting a block of data D'' at said second station using said key derived from key K'_1 to generate a message V_i'';
   (j) providing the plain text of said block D'' at said first station;
   (k) transmitting said message V_i'' to said first station;
   (l) decrypting said message V_i'' at said first station using said key derived from key K_1 to obtain a block of data D''';
   (m) comparing said data D''' and data D'' to verify synchronization at said first station.

11. The method of claim 9 wherein said predetermined manner of generating further comprises expanding K_1 and K'_1 in a predetermined manner at each of said stations, to form identical keys K_2 and K'_2.

12. The method of claim 11 further comprising modifying K_2 and K'_2 at each of said stations to generate keys for encryption and decryption of said blocks D and D' by encrypting identical variable data with K_2 and K'_2.

13. The method of claim 12 wherein said step of encrypting identical variable data comprises encrypting data identifying said first station.

14. Apparatus for generating encryption keys for a sequence of messages comprising:
   (a) means for determining a sequence of N different encryption keys;
   (b) means for associating a value of a sequence variable, T_i, with each of said messages; and

(c) means for selecting one of said N encryption keys as a function of said variable T_i for each of said messages and encrypting at least a portion of each of said messages in accordance with an encryption key derived in a predetermined manner from the corresponding one of said selected keys; said selecting means further comprising,

(d) means for selecting one of said N encryption keys so as to produce results identical to the steps of:

(d1) storing a fixed master key K_0;

(d2) storing a permutation table, said table having C columns and N rows, the columns of said table sequentially corresponding to the element positions of key K_0, the elements of said table consisting of numbers from 1 to C and

(d3) selecting a row N_i of said table in accordance with said variable T_i; and

(d4) selecting key K_0 to derive an encryption key K_1, having C elements, by, for all elements of K_1, setting the jth element of K_1 equal to the yth element of K_0, where y is the number at column j row N_i of said permutation table, where j is an integral variable ranging from 1 to C.

15. The apparatus of claim 14 further comprising means for expanding K_1 in a predetermined manner to derive an expanded encryption key K_2.

16. The apparatus of claim 15 further comprising means for modifying K_2 to form an encryption key K_3, said modifying means comprising means for encrypting variable data with K_2 to generate K_3.

17. The apparatus of claim 16 wherein said means for encrypting variable data comprises for encrypting a sequence dependent variable.

18. The apparatus of claim 15 further comprising means for modifying K_2 to form an encryption key K_3, said modifying means comprising means for encrypting variable data with K_2 to generate K_3.

19. The apparatus of claim 18 wherein said means for encrypting variable data comprises means for encrypting a sequence dependent variable.

20. The apparatus of claim 14 further comprising means for storing said permutation table in complete form.

* * * * *

US005517567A

United States Patent [19]

Epstein

[11] Patent Number: 5,517,567

[45] Date of Patent: May 14, 1996

[54] **KEY DISTRIBUTION SYSTEM**

[75] Inventor: **Philip Epstein**, Warren, N.J.

[73] Assignee: **DAQ Electronics Inc.**, Piscataway, N.J.

[21] Appl. No.: **294,626**

[22] Filed: **Aug. 23, 1994**

[51] **Int. Cl.**[6] **H04L 9/08**; H04L 9/32

[52] **U.S. Cl.** **380/21**; 380/23

[58] **Field of Search** 380/21, 23

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,731,840	3/1988	Mniszewski et al. .	
4,850,017	7/1989	Matyas, Jr. et al. .	
4,864,615	9/1989	Bennett et al.	380/21
4,876,716	10/1989	Okamoto .	
4,933,971	6/1990	Bestock et al. .	
4,944,007	7/1990	Austin .	
5,029,207	7/1991	Gammie .	
5,124,117	6/1992	Tatebayashi et al. .	
5,136,642	8/1992	Kawamura et al. .	
5,144,667	9/1992	Pogue, Jr. et al. .	
5,146,497	9/1992	Bright .	
5,146,498	9/1992	Smith .	
5,150,408	9/1992	Bright .	
5,159,633	10/1992	Nakamura .	
5,164,986	11/1992	Bright .	
5,173,938	12/1992	Steinbrenner et al. .	
5,177,791	1/1993	Yeh et al. .	
5,202,922	4/1993	Iijima	380/21 X
5,319,710	6/1994	Atalla et al.	380/23
5,392,356	2/1995	Konno et al.	380/23

Primary Examiner—Gilberto Barrón, Jr.

Attorney, Agent, or Firm—Lerner, David, Littenberg, Krumholz & Mentlik

[57] **ABSTRACT**

A system for securely distributing a communications key from a master unit to a remote unit for use in cryptographic communications between the master and remote units employs first and second secret numbers stored in both the master and remote units, and a random number generated in the master unit which is combined with the first secret number to produce a first intermediate number which is in turn combined with the second secret number to produce a second intermediate number. The second intermediate number is combined with the communications key to produce a transmission number sent with the random number to the remote unit. The remote unit, using the random number, the transmission number, and the first and second secret numbers, is able to reproduce the communications key. A method for securely distributing the communications key from the master unit to the remote unit is also provided along with a system and method for authenticating the identity of any one of a plurality of remote units in communication with the master unit, whereby each remote unit stores first and second secret numbers unique to it, all of which secret numbers are also stored in the master unit.

31 Claims, 5 Drawing Sheets

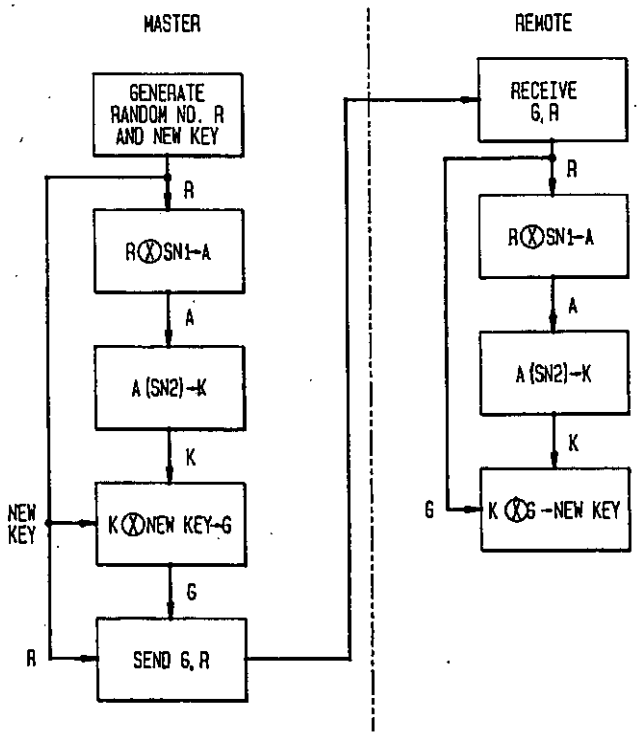


FIG. 1
(PRIOR ART)

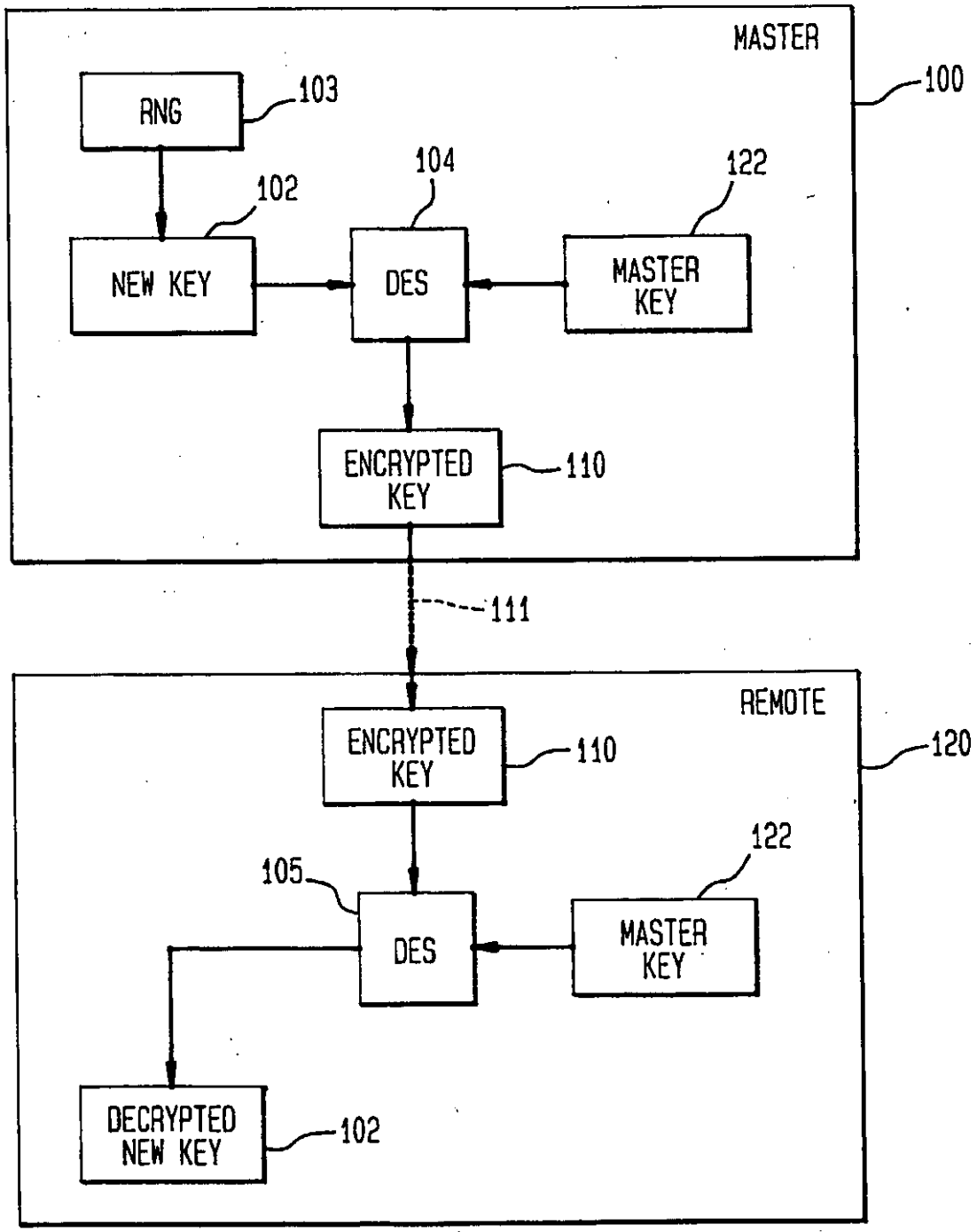


FIG. 2

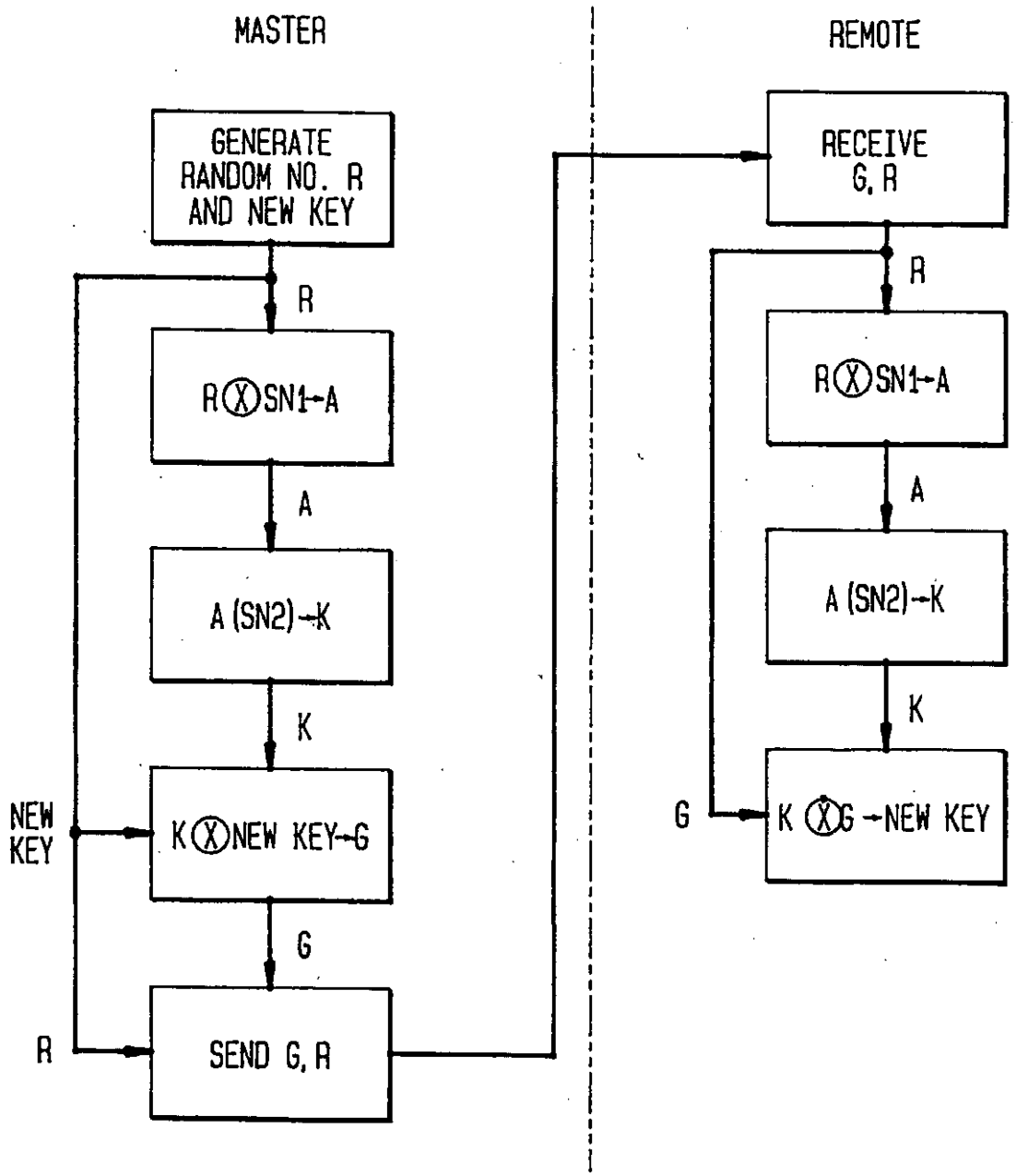

MASTER
REMOTE
GENERATE RANDOM NO. R AND NEW KEY
R
R ⓧ SN1→A
A
A (SN2)→K
K
NEW KEY
K ⓧ NEW KEY→G
G
R
SEND G, R
RECEIVE G, R
R
R ⓧ SN1→A
A
A (SN2)→K
K
G
K ⓧ G →NEW KEY

FIG. 3

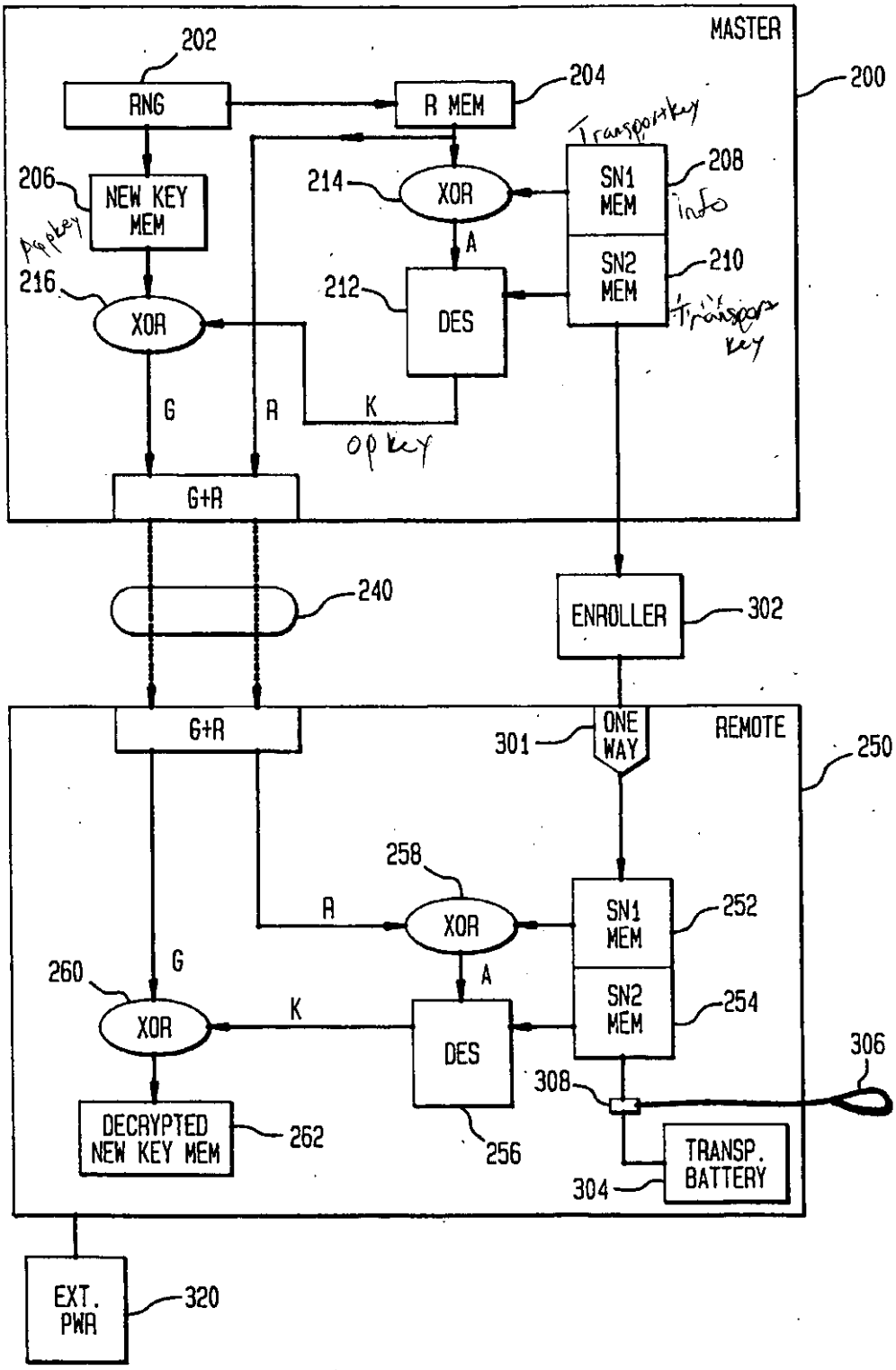

MASTER
200
202
RNG
204
R MEM
206
NEW KEY MEM
214
XOR
208
SN1 MEM
210
SN2 MEM
212
DES
216
XOR
G
R
K
A
G+R
240
ENROLLER
302
REMOTE
250
301
ONE WAY
258
XOR
252
SN1 MEM
254
SN2 MEM
260
XOR
DES
256
306
308
DECRYPTED NEW KEY MEM
262
TRANSP. BATTERY
304
EXT. PWR
320

FIG. 4

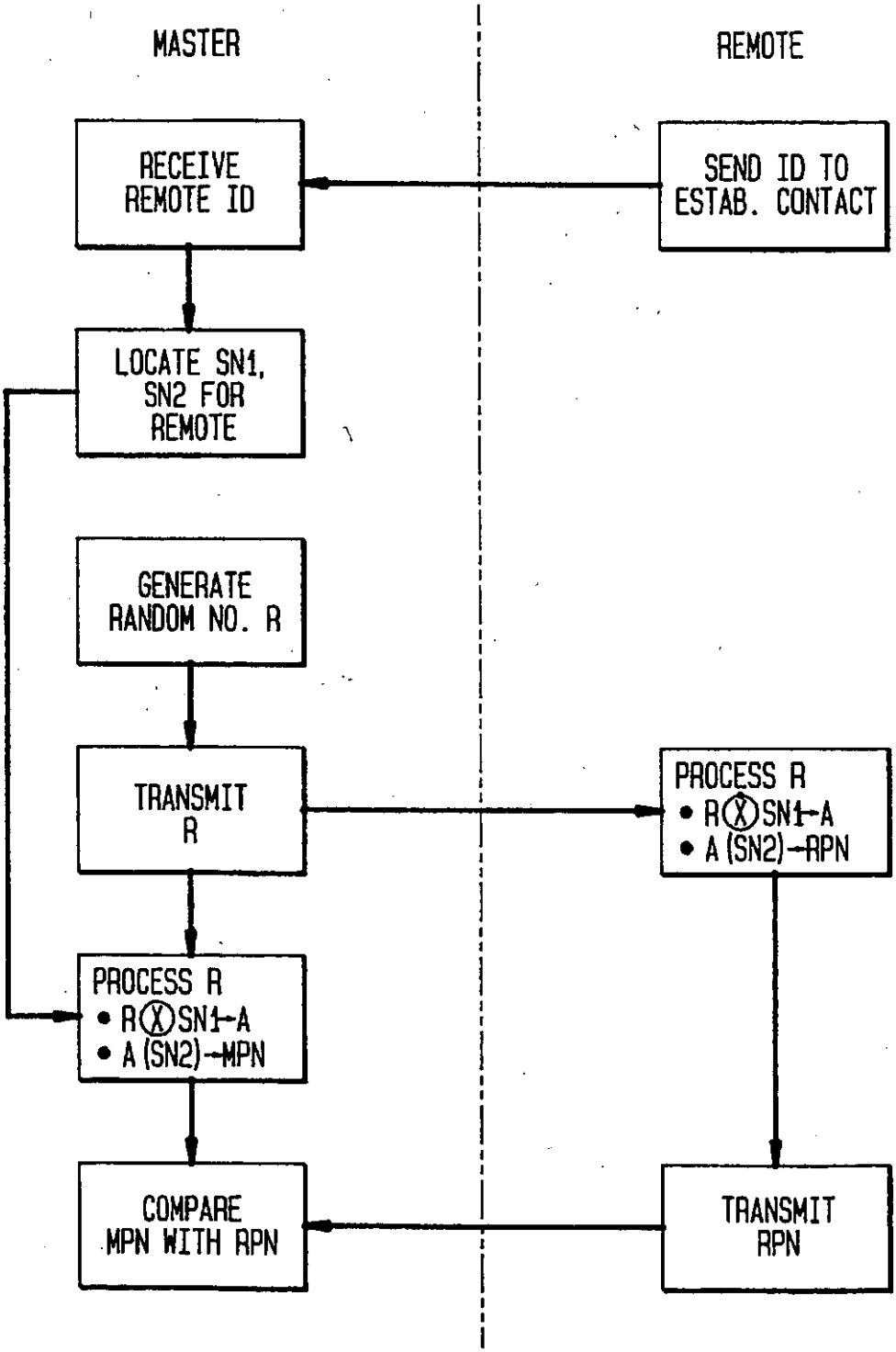
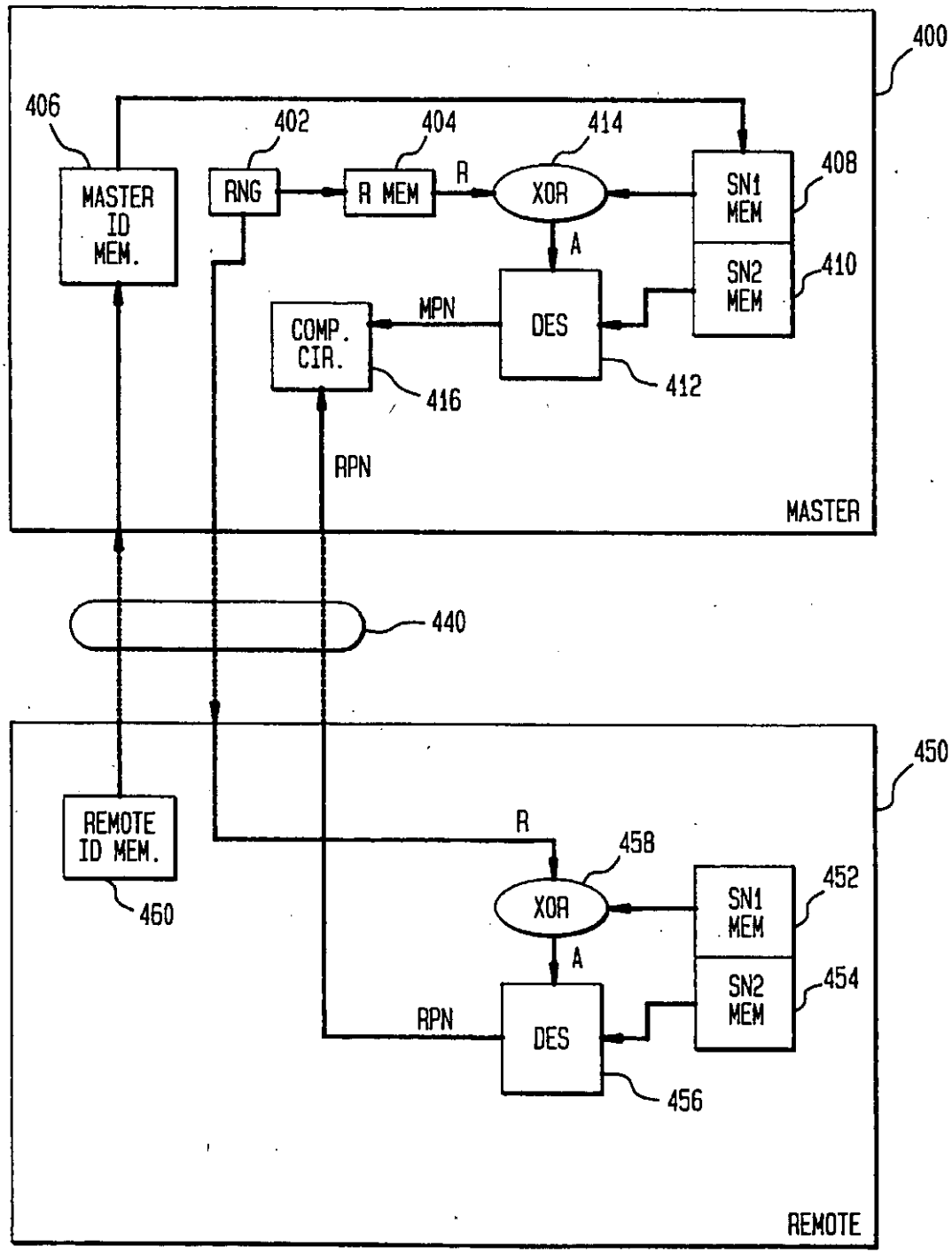

MASTER
REMOTE
RECEIVE REMOTE ID
SEND ID TO ESTAB. CONTACT
LOCATE SN1, SN2 FOR REMOTE
GENERATE RANDOM NO. R
TRANSMIT R
PROCESS R
• R⊗SN1→A
• A (SN2)→RPN
PROCESS R
• R⊗SN1→A
• A (SN2)→MPN
COMPARE MPN WITH RPN
TRANSMIT RPN

FIG. 5


400
406
402
404
414
408
MASTER ID MEM.
RNG
R MEM
R
XOR
SN1 MEM
A
SN2 MEM
410
MPN
DES
COMP. CIR.
412
416
RPN
MASTER
440
450
REMOTE ID MEM.
460
R
458
XOR
452
SN1 MEM
A
SN2 MEM
454
RPN
DES
456
REMOTE

KEY DISTRIBUTION SYSTEM

FIELD OF THE INVENTION

This invention relates to a system and method for securely distributing a communications key from a master system to a remote system for use in cryptographic communications between the master and remote systems.

BACKGROUND OF THE INVENTION

In today's age of communications, the use of cryptography is becoming increasingly important to protect confidential communications between a sender and a receiver transmitted over public or easily accessible communications channels such as telephone lines, satellite links, wireless networks, cellular phone systems, etc. The basic idea of cryptography is to first scramble or encrypt the private message, and then send the encrypted message over the communications channel to the receiver where the message is then decrypted and read. If the encrypted message is intercepted by an unauthorized party and cannot be decrypted, it will be unintelligible.

In key-based encryption systems, the message to be sent is encrypted with a "key" or "communications key" which is a code known only to the sender and receiver and is not known to other unauthorized parties who may try to intercept the encrypted message. If the sender and receiver possess and agree to use the same key, the sender can encrypt the message with the communications key and send the unintelligible, encrypted message over the communications channel to the receiver, who can then decrypt the message using the same communications key used by the sender to encrypt the message.

In 1977, the United States National Bureau of Standards decided on a defined encryption algorithm known as the Data Encryption Standard (DES), which is now the standard for the encryption of certain classes of data. DES encryption is currently used by federal agencies as well as by private companies in areas such as electronic banking and money transfer. DES encryption works with a user-supplied data encryption key with a word length of 56 bits. The encryption key, which must be known by both the sender and receiver of the message, is used to encrypt the message, which then appears as an apparently random sequence of unintelligible bits. Since both the encryption and decryption procedures used with DES are publicly known, maintaining the secrecy of the encryption key is imperative when using any DES encryption system. Today there are commercially available integrated circuits which can implement the DES encryption and decryption procedure.

As with DES encryption, one of the largest problems encountered in any key-based encryption system is the need to keep the key secure. One solution is to frequently update the communications key such that even if one key is recovered by an unauthorized user, a subsequent key change will not allow decryption of subsequent messages. To this end, many different methods of key distribution have been devised.

In one widely-used method of key distribution, a human courier or "trusted friend" can be used to physically distribute new keys to the remote systems on a periodic basis. This method can be problematic, however, if the confidence of the trusted friend is compromised or the key is intercepted along the way by an unauthorized party.

Another type of key distribution system is known as a public key system in which the communications key need not be physically distributed or even agreed on in advance by the sender and receiver. In such a system, User A publishes a public encoding key E_A to all users of the system and keeps private a decoding key D_A, whereby $D_A(E_A(M))=M$, where M is the message to be sent, $E_A(M)$ is the encryption of message M, and $D_A(E_A(M)$ is the description of encrypted message M. In such a system, however, User A must not publicly reveal D_A when showing E_A, and the decoding key D_A must not be computable from encoding key E_A. Using this system, User B, who desires to send a message to User A, can look up the encoding key E_A of User A which is published. User B then uses E_A to encrypt the message to be sent to User A. Upon receipt of the encrypted message, User A can quickly decode the message whereas other users or unauthorized parties who do not possess D_A cannot easily ascertain the message from the published E_A. This system is extremely slow, however, when used to send large messages due to its reliance on intensive computations needed to decrypt the message.

Another key distribution system, known as double encryption, is disclosed in U.S. Pat. No. 5,029,207 to Gammie. In this system, an external security module for a television signal decoder is provided in which the key to be sent is encrypted using two secret serial numbers known only to the master and the particular remote subscriber. The key used to descramble the program signal is first encrypted with the secret serial number of the remote unit's replaceable security module, and then encrypted again with the secret serial number of the remote unit's decoder. The decoder then uses its two secret serial numbers to work backwards and decrypt the key, which it then uses to descramble the program signal.

U.S. Pat. No. 5,146,498 to Smith discloses a method of remotely changing the encryption key where an original key is stored in a remote unit, and the master unit sends a signal to effectuate a key change based on operations performed on the original key. The key itself, however, is not sent, but rather the new key is generated as a result of mathematical operations on the original key initiated from a key change command sent from the master unit.

U.S. Pat. No. 4,731,840 to Mniszewski et al. discloses a method for encrypting and sending digital key data using DES encryption. Each remote unit used in the system contains a set of key-encryption keys indexed by a common system. The master unit, upon request from the remote unit, generates a key and encrypts it with a preselected key-encryption key. The encrypted key and an index designator is sent to a remote unit wherein the key is decrypted to reproduce a data encryption key.

Other systems, such as that disclosed in U.S. Pat. No. 5,159,633 to Nakamura, use combined public and secret key encryption systems. In Nakamura, storage information is encrypted with a public key system while real time transmission data such as a video signal is encrypted with a secret key system.

FIG. 1 shows another example of a prior art key encryption system that includes a central or master unit **100** and a remote unit **120**. At master unit **100**, a new key **102** is chosen by a random number generator (RNG) **103** to serve as the communications key and must be safely transferred to remote unit **120** over communications channel **111**. To this end, master unit **100** generates and then encrypts the new key **102** with a master key **122** of remote unit **120**, using DES encryption unit **104** to thereby generate encrypted key

110. Encrypted key 110 is then sent to the remote unit 120 which will then decrypt encrypted key 110 using DES encryption unit 105 and master key 122 to recover new key 102. New key 102 is then used as the new communications key for subsequent communications between master unit 100 and remote unit 120.

This system, however, is subject to attack as follows. First, the attacker intercepts and records the first message sent to remote unit 120 which contains the encrypted key 110. The attacker then records subsequent messages sent encrypted with new key 102. The attacker can then break the code on subsequent messages and recover new key 102. With new key 102 now obtained, the attacker can decrypt the first message and recover master key 122. With knowledge of master key 122, all subsequent messages are vulnerable to interception.

Other data encryption techniques are used by the cellular phone industry to protect not only communications between callers, but to protect the security of identification numbers of remote cellular phones subscribing to the particular system. However, the present systems that attempt to maintain the secrecy of the remote phone's identification number are subject to attack. Currently, when a cellular phone is used, it must first establish initial contact with the base station. When the initial contact is made, the remote cellular phone is then interrogated by the base station in order to obtain the cellular phone's identification number. This identification number is then used by the cellular phone system to invoice the customer for the call. However, attackers can intercept the initial transmission and determine the remote user's identification number, which they can then proceed to install in a cellular phone of their own which can now be used or sold. Calls made from this "imposter" phone will then be billed to the original subscriber. This type of cellular telephone fraud has swamped the phone companies with requests for new telephone numbers and for billing refunds from cellular users, resulting in the loss by the phone companies of significant amounts of money.

Accordingly, in any situation in which communication between a sender and a receiver must be kept confidential, there is a need to provide a key encryption system that is relatively easy to implement and less vulnerable to attack by unauthorized parties. There has been a long felt need to provide such an improved key encryption system which is extremely secure and nearly impossible to break and decrypt subsequent communication keys. There is also a need to provide an improved encryption system that will prevent cellular phone fraud and fraud in similar types of systems by authenticating the identity of the remote unit.

SUMMARY OF THE INVENTION

The present invention meets these above needs. According to one aspect of the present invention, there is provided a method for securely distributing a communications key from a master unit to a remote unit. The method includes the steps of:

(a) storing first and second secret numbers in the master and remote units;

(b) generating a random number and storing the random number in the master unit;

(c) combining the random number with the first secret number to produce a first intermediate number in the master unit;

(d) combining the first intermediate number with the second secret number to produce a second intermediate number in the master unit;

(e) combining the second intermediate number with the communications key to produce a transmission number in the master unit;

(f) transmitting the transmission number and the random number from the master unit to the remote unit;

(g) receiving the transmission number and the random number in the remote unit;

(h) combining the random number with the first secret number to recreate the first intermediate number in the remote unit;

(i) combining the first intermediate number with the second secret number to produce the second intermediate number in the remote unit; and

(j) combining the second intermediate number with the transmission number to produce the communications key in the remote unit.

The method preferably includes the step of combining the first intermediate number with the second secret number in the master and remote units by the step of encrypting the first intermediate number using the second secret number as the encrypting key. More preferably, this encrypting step comprises DES encryption.

In preferred methods, the step of combining the random number with the first secret number in the master and remote units includes the step of exclusive OR-ing the random number with the first secret number; the step of combining the second intermediate number with the communications key; in the master unit includes the step of exclusive OR-ing the intermediate number with the communications key; and the step of combining the second intermediate number with the transmission number in the remote system includes the step of exclusive OR-ing the second intermediate number with the transmission number.

Preferably, steps (b) through (j) are repeated on a periodic basis to change the communications key, with a preferred periodic basis being about every hour, or more preferably less than every 15 minutes, or most preferably, every three minutes. The method may also include the step of securely loading the first and second secret numbers from the master system to the remote unit.

The present invention also provides a system for performing the method. A still further aspect of the present invention provides a method for authenticating the identity of a remote unit in a plurality of remote units in communication with a master unit, where the master and remote units have stored therein first and second secret numbers identifying the remote unit. The authenticating method includes the steps of:

(a) storing in each one of the plurality of remote units first and second secret numbers, the first and second secret numbers in one remote unit being different than the first and second secret numbers in any other remote unit;

(b) storing in the master unit the first and second secret numbers of the plurality of the remote units;

(c) establishing initial contact between the master unit and a selected one of the plurality of the remote units;

(d) providing a random number to the master unit;

(e) transmitting the random number from the master unit to the selected remote unit;

(f) processing the random number in the selected remote unit with the first and second secret numbers to generate a remote processed number;

(g) processing the random number in the master unit with the first and second secret numbers to generate a master processed number;

(h) transmitting the remote processed number to the master unit; and

(i) comparing the remote processed number and the master processed number in the master unit, wherein the identity of the selected remote unit is authenticated when the remote processed number is equal remote unit is authenticated when the remote processed number is equal to the master processed number.

Preferably, the step of processing the random number in the selected remote unit includes the steps of combining the random number with the first secret number to generate a remote intermediate number and combining the remote intermediate number with the second secret number to generate the remote processed number. Further, the step of processing the random number in the master unit may include the steps of combining the random number with the first secret number to generate a master intermediate number and combining the master intermediate number with the second secret number to generate the master processed number.

The step of combining the random number with the first secret number in the selected remote and master units preferably includes the step of exclusive OR-ing the random number with the first secret number in the master and selected remote units. Also preferably, the remote and master intermediate numbers are combined with the second secret number by an encrypting step using the second secret number as the encrypting key. In a highly preferred method, the encrypting step is conducted using DES encryption.

The step of establishing initial contact may further include the step of transmitting an identification number from the selected remote unit to the master unit and recalling in the master unit the first and second secret numbers associated with that identification number.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is an example of a prior art key distribution system;

FIG. **2** is a flow chart illustrating a method of key distribution in accordance with one aspect of the present invention;

FIG. **3** is a schematic diagram of a key distribution system for performing the method of FIG. **2**;

FIG. **4** is a flow chart illustrating a method for authenticating the identity of a remote unit in communication with a master unit in accordance with another aspect of the present invention; and

FIG. **5** is a schematic diagram of an authentication system for performing the method of FIG. **4**.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to FIG. **3**, a schematic diagram of a key distribution system in accordance with the present invention is illustrated. The key distribution system includes a master unit **200** and a remote unit **250** which, after installation and set up, are in communication with one another through communications channel **240**. Communications channel **240** can comprise many different forms such as regular telephone lines, satellite links, local area networks, free space transmission, etc.

Master unit **200** includes a random number generator (RNG) **202** for generating a random number R, preferably of 8 bytes, which is stored in R memory **204**. Random number generator **202** is also used to generate a random number, preferably of 8 bytes, to be used as the new communications key which is stored in new key memory **206**. Master unit **200** is further provided with secret number (SN) memories SN1 memory **208** for storing a first secret number SN1, and SN2 memory **210** for storing a second secret number SN2. Secret numbers SN1 and SN2 preferably have a length of 8 bytes each. Master unit **200** also includes a conventional DES encryption unit **212**, such as DES unit Am9518 sold by Advanced Micro Devices of Sunnyvale, Calif., and XOR (exclusive-OR) gates **214** and **216**. A single XOR gate may also be used in master unit **200** for all necessary XOR operations.

Remote unit **250** of the key distribution system likewise includes SN1 and SN2 memories **252** and **254** for storing first and second secret numbers SN1 and SN2, respectively, conventional DES encryption unit **256**, XOR gates **258** and **260** (which can be combined into one gate) and decrypted new key memory **262**. Remote unit **250** also includes one way data port **301** connected to SN1 and SN2 memories **252** and **254**. Transport battery **304** is also provided within remote unit **250** and is connected to SN1 and SN2 memories **252** and **254**. An arming lanyard **306** is connected to node **308** and when released will disengage transport battery **304** from SN1 and SN2 memories **252** and **254**. When installed in its intended location, remote unit **250** is powered by external power supply **320**.

The operation of the key distribution system shown in FIG. **3** is as follows. Initially, prior to any key changes, remote unit **250** is "enrolled" with its secret number pair SN1 and SN2. Master unit **200** likewise is initially provided with the same two secret numbers SN1 and SN2. To enroll remote unit **250**, secret numbers SN1 and SN2 are first loaded in SN1 and SN2 memories **208** and **210**, respectively, of master unit **200**. Secret numbers SN1 and SN2 may be retrieved from a secret number memory bank (not shown) containing secret number pairs of all remote units used in the system. SN1 and SN2 then may be enrolled into SN1 and SN2 memories **252** and **254** in remote unit **250** before remote unit **250** is taken to the remote site. In order to enroll remote unit **250** with its secret numbers SN1 and SN2, an enroller **302** may be provided to allow SN1 and SN2 to be securely read out from SN1 and SN2 memories **208** and **210** in master unit **200** and into SN1 and SN2 memories **252** and **254** of remote unit **250**.

Enroller **302** preferably consists of a cable and plug and connects master unit **200** with remote unit **250** only during the enrolling process. Remote unit **250** is provided with a one-way data transfer port **301**, such as an ASCII port used only for enrolling the remote unit **250**. One-way transfer port **301** provides additional security by not allowing SN1 and SN2 or any other data to be read out through that port.

After remote unit **250** is enrolled, SN1 and SN2 are stored in SN1 and SN2 memories **252** and **254**, which consist of volatile memory. While taking remote unit **250** to its intended remote installation location, volatile SN1 and SN2 memories **252**, **254** are temporarily maintained by way of transport battery **304** since remote unit **250** is not yet connected to external power supply **320**. Transport battery **304**, however, is detachable from memories **252** and **254** by the removal of arming lanyard **306** which breaks the transport battery connection at node **308** once remote unit **250** is securely installed in its remote location and connected to external power supply **320**. Thus, once remote unit **250** is installed at its intended remote location and arming lanyard **306** is removed, any attempts to remove remote unit **250** from its installed location will cut off external power supply **320** and will result in the immediate loss of all memory

including SN1 and SN2. For further security, remote unit **250** is preferably provided with a tamper-proof housing such that any attempt to physically penetrate remote unit **250** without removing it will also cut off the external power supply and destroy all memory.

Once remote unit **250** is enrolled with SN1 and SN2 and installed in its intended remote location, the new communications key is generated and distributed as follows. In master unit **200**, random number generator **202** first generates a new key which is then stored in new key memory **206**. Random number generator **202** also generates a random number R which is stored in R memory **204**. Random number R and SN1 are then sent to XOR gate **214** and XOR-ed to produce a first intermediate number A. First intermediate number A is then encrypted by DES encryption unit **212** using SN2 as the encryption key, thereby generating a second intermediate number K. Second intermediate number K is then XOR-ed at XOR gate **216** with the new communications key stored in new key memory **206** to generate a transmission number G in master unit **200**. Transmission number G is then sent together with random number R over communications channel **240**, e.g., over a phone line, satellite link, etc., to remote unit **250**.

At remote unit **250**, the process is then reversed in order to recreate the new communication key to be used. In this regard, transmission number G and random number R are initially received from master unit **200**. Random number R is then XOR-ed with SN1 at XOR gate **258** to recreate first intermediate number A. First intermediate number A is then encrypted at DES encryption unit **256** using secret number SN2 as the encryption key. The result of the encryption operation is the recreation of second intermediate number K, which is then XOR-ed with transmission number G at XOR gate **260** in order to decrypt and recreate the new communications key, which subsequently may be stored in decrypted new key memory **262**. Once remote unit **250** has recovered the new communications key, remote unit **250** and master unit **200** may safely communicate with one another other by encrypting messages with the common communications key known only to the master and remote units.

The advantage of this key distribution system lies in the fact that a new communications key can be sent as often as desired from the master unit to the remote unit, and even if an unauthorized party can somehow manage to decipher the particular key in use, knowing that key will not yield the first and second secret numbers SN1 and SN2 which are unique to each remote unit and used in all key changes. As a result, a new key can be distributed with such a high frequency that it would not be useful to attempt to decrypt the key since that key will shortly be changed and thereafter will be useless. Therefore, in order to break the system, a would-be attacker would have to attempt to obtain the two secret numbers. The new key is preferably distributed on a periodic basis about every hour, and more preferably less than every 15 minutes. Most preferably, the new key is distributed about every three minutes.

Assuming that the would-be attacker is even able to determine the second intermediate number K, it is virtually impossible to obtain both secret numbers. Knowing K, the attacker would have to find two numbers (secret numbers SN1 and SN2) such that SN1 XOR-ed with R and then encrypted using SN2 as the key, will yield intermediate number K. The problem is that there are 2^{120} possible combinations of which no less than 256 appear to work since SN1 XOR-ed with R and encrypted using SN2 will yield the communications key when tested against the message. However, only one of these 256 combinations is actually correct, and only the correct combination will work with subsequent key changes. Since a new communications key is preferably transmitted every few minutes, it is virtually impossible for the attacker to break the system.

Although FIG. **3** only illustrates a single remote unit, it should be appreciated that multiple remote units may be used in the system, with each remote unit having its own unique secret numbers SN1 and SN2 which can be ascertained in the master unit when the master unit effectuates a key change to each remote unit.

The key encryption system of the present invention is useful not only to protect communications between a sender and a receiver where the primary consideration is concealing the content of the message being sent, but is also extremely useful in security systems where the content of the message is typically known. Such "messages", including card swipes, the opening of doors, etc., must be protected from being aliased, i.e., false messages being sent to deceive the master unit.

Referring now to FIG. **2**, a flow chart of the method of the present invention is shown. As can be seen, a random number R is first generated in the master unit and then XOR-ed with SN1 to produce first intermediate number A. First intermediate number A is then encrypted with SN2 (by DES encryption) to produce second intermediate number K. Second intermediate K is then XOR-ed with the new key to be sent to produce the transmission number G. The master unit then sends transmission number G and random number R to the remote unit. The remote unit then reverses the sequence by XOR-ing random number R with SN1 to recreate first intermediate number A. First intermediate number A is then encrypted with SN2 (by DES encryption) to produce second intermediate number K. Second intermediate number K is then XOR-ed with transmission number G to recreate the new communications key to be used in subsequent communications. Preferably, a new key is sent out as frequently as necessary, such as every three minutes, other predetermined periodic time intervals such as every **15** minutes or every hour, or even at random time intervals.

Turning now to FIG. **5**, a system for authenticating the identity of each remote unit, such as a cellular telephone unit in a system of remote units in communication with a master unit, is shown in schematic form. The identification system includes a master unit **400** and at least one remote unit **450** which are in communication with one another through communication channel **440**.

Master unit **400** includes a random number generator **402** for generating a random number R which can be stored in R memory **404**. Master unit **400** is further provided with secret number (SN) memories SN1 memory **408** for storing first secret number SN1, and SN2 memory **410** for storing second secret number SN2. Secret number pairs SN1 and SN2 are provided for each remote unit **450**, and therefore, master unit **400** can include a master ID memory **406** to store all of the secret numbers SN1 and SN2 for each remote unit in the system. Master unit **400** also includes a conventional DES encryption unit **412**, XOR gate **414**, and comparison circuit **416** used for comparing a pair of numbers to determine whether they are the same.

Each remote unit of the identification system, such as remote unit **450**, includes SN1 and SN2 memories **452** and **454** for storing first and second secret numbers SN1 and SN2, unique to that remote unit respectively. Remote unit **450** also includes a conventional DES encryption unit **456**, XOR gate **458** and remote ID memory **460** which stores the unique identification number of the particular remote unit in the system.

The operation of the system shown in FIG. 5 for authenticating the identity of each remote unit in the system is as follows. Master unit **400** is initially provided with all of the pairs of secret numbers, SN1 and SN2, for all of the remote units in the system. These secret numbers are stored in remote ID memory **406**. The secret numbers of each remote system may then be enrolled into SN1 and SN2 memories **452** and **454** of each remote unit. In this manner, remote unit **450**, for example, can be enrolled with its unique secret numbers SN1 and SN2 as previously explained in the key distribution system of the present invention, i.e., by providing a one way transfer port in remote unit **450** for one way downloading of the secret numbers SN1 and SN2. In addition, remote unit **450** may also be provided with additional security measures as described above in the key distribution system, including volatile memory **452** and **454** maintained only by way of a transport battery, the connection to which can be broken by the use of an arming lanyard or similar device once remote unit **450** is connected to an external power supply, such as a car battery. In this manner, remote unit **450** should also be tamper-proof such that any attempts to ascertain SN1 and SN2 will result in the immediate loss of these numbers from memory.

After remote unit **450** is enrolled with SN1 and SN2 and installed in its intended remote location, initial contact must be established between master unit **400** and remote unit **450**. For example, in a cellular phone system, this could be established when the sender of the call from remote unit **450** initially dials and sends a telephone number. With the telephone number, remote unit **450** can send its unique identification number, stored in ID memory **460**, which will then be received in master unit **400**. Once master unit receives the identification number, it then can look up the secret numbers SN1 and SN2 for remote unit **450** as identified by its unique identification number. With SN1 and SN2 of the remote unit **450**, random number generator **402** generates a random number R which is stored in R memory **404**. Random number R is then sent from master unit **400** to remote unit **450** in which it is received and XOR-ed with SN1 at XOR gate **458**. This XOR operation produces a first intermediate number A which is then encrypted by DES unit **456**, using SN2 as the encryption key, to thereby generate a remote processed number RPN.

At the same time, in the master unit **400** the same random number R is likewise XOR-ed with SN1 at XOR gate **414** producing intermediate number A, which is in turn encrypted by DES unit **412** using SN2 as the encryption key. The result is a master processed number MPN. The remote unit **450** then transmits RPN to master unit **400** where it is compared with MPN at comparison circuit **416**, such as by the use of one or more XOR gates in order to determine whether they match. If MPN equals RPN, then the remote unit is authenticated and the call is allowed to proceed.

Turning to FIG. **4**, a flow chart of the method of authenticating the identity of a remote unit is shown. Thus, initial contact is first established between the master and remote units and the identification number of the remote unit is sent to the master unit. The master unit then uses the identification number to locate SN1 and SN2 for the identified remote unit. Next, a random number R is generated in the master unit which is then transmitted to the remote system. The remote unit, which already has stored first and second secret numbers SN1 and SN2, processes random number R using these secret numbers to generate a remote processed number RPN.

The same processing of the random number R occurs in the master unit using the secret numbers SN1 and SN2 of the identified remote unit. The remote unit then transmits the remote processed number RPN to the master unit where the master processed number MPN is compared to the remote processed number RPN to authenticate the identity of the remote unit. If RPN and MPN match, then the remote unit is authentic since only the remote unit will be able to recreate a remote processed number equal to the master processed number by the use of secret numbers SN1 and SN2.

Preferably, the processing of the random number in both the master and remote units is accomplished by first XORing random number R with SN1 to produce an intermediate number A, although other logical and arithmetic operations may be used, such as multiplication and truncation, so long as the same operation is performed both in the master and remote units, or if different operations are used, so long as the differences in the operations are accounted for in the master and/or remote units. Intermediate number A is, in turn, encrypted using SN2, preferably using DES encryption, to generate the remote and master processed numbers for comparison.

It should be apparent to those of ordinary skill in the art that all of the operations described herein can be carried out under the control of a microprocessor or CPU and using readily available electronic and IC components. Moreover, although DES encryption is preferred for encrypting operations in accordance with the present invention, other encrypting operations can be used, such as matrix, table look-up, etc.

Although the invention herein has been described with reference to particular embodiments, it is to be understood that these embodiments are merely illustrative of the principles and applications of the present invention. It is therefore to be understood that numerous modifications may be made to the illustrative embodiments and that other arrangements may be devised without departing from the spirit and scope of the present invention as defined by the appended claims.

What is claimed is:

1. A system for securely distributing a communications key from a master unit to a remote unit, comprising:

memory means for storing first and second secret numbers in the master unit;

random number generating means for providing a random number to the master unit;

first combining means in the master unit for combining said random number with said first secret number to produce a first intermediate number;

second combining means in the master unit for combining said first intermediate number with said second secret number to produce a second intermediate number;

third combining means in the master unit for combining said second intermediate number with the communications key to produce a transmission number;

communication means for transmitting signals between the master and remote units;

memory means for storing said first and second secret numbers in the remote unit;

first combining means in the remote unit for combining said random number with said first secret number to produce said first intermediate number;

second combining means in the remote unit for combining said first intermediate number with said second secret number to produce said second intermediate number; and

third combining means in the remote unit for combining said intermediate number with said transmission number to produce the communications key.

2. The system as claimed in claim 1, wherein said second combining means in the master unit and said second combining means in the remote unit include encryption means for encrypting said first intermediate number using said second secret number as an encrypting key.

3. The system as claimed in claim 2, wherein said encryption means uses DES encryption.

4. The system as claimed in claim 1, wherein said first combining means in the master unit and said first combining means in the remote unit include means for exclusive OR-ing said random number with said first secret number.

5. The system as claimed in claim 1, wherein said third combining means in the master unit includes means for exclusive OR-ing said second intermediate number with the communications key and said third combining in the remote unit includes means for exclusive OR-ing said second intermediate number with said transmission number.

6. The system as claimed in claim 4, wherein said third combining means in the remote unit includes means for exclusive OR-ing said second intermediate number with said transmission number.

7. The system as claimed in claim 1, further comprising enrolling means for securely copying said first and second secret numbers from the master unit into said memory means in the remote unit.

8. A method for securely distributing a communications key from a master unit to a remote unit, comprising the steps of:

(a) storing first and second secret numbers in the master and remote units;

(b) generating a random number and storing said random number in the master unit;

(c) combining said random number with said first secret number to produce a first intermediate number in the master unit;

(d) combining said first intermediate number with said second secret number to produce a second intermediate number in the master unit;

(e) combining said second intermediate number with said communications key to produce a transmission number in the master unit;

(f) transmitting said transmission number and said random number from the master unit to said the remote unit;

(g) receiving said transmission number and said random number in the remote unit;

(h) combining said random number with said first secret number to produce said first intermediate number in the remote unit;

(i) combining said first intermediate number with said second secret number to produce said second intermediate number in the remote unit; and

(j) combining said second intermediate number with said transmission number to produce said communications key in the remote unit.

9. The method as claimed in claim 8, wherein said step of combining said first intermediate number with said second secret number in the master and remote units includes the step of encrypting said first intermediate number using said second secret number as an encrypting key.

10. The method as claimed in claim 9, wherein said encrypting step comprises DES encryption.

11. The method as claimed in claim 8, wherein said step of combining said random number with said first secret number in the master and remote units includes the step of exclusive OR-ing said random number with said first secret number.

12. The method as claimed in claim 8, wherein said step of combining said second intermediate number with said communications key in the master unit includes the step of exclusive OR-ing said second intermediate number with said communications key and said step of combining said second intermediate number with said transmission number in the remote unit includes the step of exclusive OR-ing said second intermediate number with said transmission number.

13. The method as claimed in claim 11, wherein said step of combining said second intermediate number with said communications key in the master unit includes the step of exclusive OR-ing said second intermediate number with said communications key and said step of combining said second intermediate number with said transmission number in the remote unit includes the step of exclusive OR-ing said second intermediate number with said transmission number.

14. The method as claimed in claim 8, wherein said steps of (b) through (j) are repeated on a periodic basis to change said communications key.

15. The method as claimed in claim 14, wherein said periodic basis is about every hour.

16. The method as claimed in claim 14, wherein said periodic basis is less than every 15 minutes.

17. The method as claimed in claim 14, wherein said periodic basis is about every three minutes.

18. The method as claimed in claim 8, further including the step of securely copying said first and second secret numbers from the master unit to the remote unit.

19. A method for authenticating the identity of remote unit in a plurality of remote units in communication with a master unit, said method comprising the steps of:

(a) storing in each one of the plurality of remote units first and second secret numbers, said first and second secret numbers in one remote unit being different than said first and second secret numbers in any other remote unit;

(b) storing in the master unit said first and second secret numbers of the plurality of the remote units;

(c) establishing initial contact between the master unit and a selected one of the plurality of remote units;

(d) providing a random number to the master unit;

(e) transmitting said random number from the master unit to said selected remote unit;

(f) processing said random number in said selected remote unit with said first and second secret numbers stored in said selected remote unit to generate a remote processed number;

(g) processing said random number in the master unit with said first and second secret numbers to generate a master processed number;

(h) transmitting said remote processed number to the master unit; and

(i) comparing said remote processed number and said master processed number in the master unit, whereby the identity of said selected remote unit is authenticated when said remote processed number is equal to said master processed number.

20. A method as claimed in claim 19, wherein said step of processing said random number in said selected remote and master units comprises the steps of combining said random number with said first secret number to generate an inter-

mediate number and combining said intermediate number with said second secret number to generate said respective remote and master processed numbers.

21. The method as claimed in claim 20, wherein said step of combining said random number with said first secret number in said selected remote unit and the master unit includes the step of exclusive OR-ing said random number with said first secret number in the master unit and said selected remote unit.

22. A method as claimed in claim 20, wherein said step of combining said intermediate number with said second secret number in the master unit and said selected remote unit includes the step of encrypting said intermediate number using said second secret number as an encrypting key.

23. The method as claimed in claim 22, wherein said encrypting step comprises DES encryption.

24. The method as claimed in claim 19, wherein said step of establishing initial contact comprises the steps of transmitting an identification number from said selected remote unit to the master unit and recalling in the master unit said first and second secret numbers associated with said identification number identifying said selected remote unit.

25. A system for authenticating the identity of a remote unit in a plurality of remote units in communication with a master unit, comprising:

remote memory means for storing in each one of the plurality of remote units first and second secret numbers, said first and second secret numbers in one remote unit being different than said first and second secret numbers in any other remote unit;

master memory means for storing in the master unit said first and second secret numbers of the plurality of the remote units;

contact means for establishing initial communication between the master unit and a selected one of the plurality of said remote units;

random number generating means for providing a random number to the master unit;

communications means for transmitting signals between the master and remote units;

remote processing means for combining said random number in said selected remote unit with said first and second secret numbers stored in said selected remote unit in said predetermined manner to generate a remote processed number;

master processing means for processing said random number in the master unit with said first and second secret numbers for said selected remote unit stored in the master unit in said predetermined manner to generate a master processed number; and

comparison means for comparing said remote processed number and said master processed number in the master unit, whereby the identity of said selected remote unit is authenticated when said remote processed number is equal to said master processed number.

26. The system as claimed in claim 25, wherein said remote processing means and said master processing means comprise first combining means for combining said random number with said first secret number to produce an intermediate number and means for combining said intermediate number with said second secret number to produce said respective remote and master processed numbers.

27. The system as claimed in claim 26, wherein said first combining means in said selected remote and master units include means for exclusive OR-ing said random number with said first secret number.

28. The system as claimed in claim 26, wherein said second combining means in said selected remote and master units include encryption means for encrypting said intermediate number using said second secret number as an encrypting key.

29. The system as claimed in claim 28, wherein said encryption means uses DES encryption.

30. The system as claimed in claim 25, wherein said contact means comprises transmission means for transmitting an identification number from said selected remote unit to the master unit.

31. The system as claimed in claim 25, wherein said selected remote unit comprises a cellular telephone.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 5,517,567
DATED : May 14, 1996
INVENTOR(S) : Epstein

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 7, line 64, "256" should read --2^{56}--.

Column 7, line 67, "256" should read --2^{56}--.

Signed and Sealed this

Thirteenth Day of August, 1996

Attest:

BRUCE LEHMAN

Attesting Officer

Commissioner of Patents and Trademarks